UNSOLVED PROBLEMS

Edited by: **Richard Guy**

In this department the MONTHLY presents easily stated unsolved problems dealing with notions ordinarily encountered in undergraduate mathematics. Each problem should be accompanied by relevant references (if any are known to the author) and by a brief description of known partial or related results. Typescripts should be sent to Richard Guy, Department of Mathematics & Statistics, The University of Calgary, Alberta, Canada T2N 1N4.

When Does a Polynomial over a Finite Field Permute the Elements of the Field?, II

Rudolf Lidl and Gary L. Mullen

In [**16**] we provided a brief survey of the main known classes of **permutation polynomials** (PPs) over finite fields, ($f \in F_q[x]$ is a PP if f induces a 1–1 mapping on F_q where F_q is the finite field of order q, with q a prime power). In addition, nine problems concerning PPs were discussed in [**16**] and as a result it seems that [**16**] has at least partly motivated a number of subsequent papers [**2–5**, **7**, **9–11**, **23–25**] in which various aspects of PPs have been considered.

Progress has recently been made on a number of the problems raised in [**16**] and so it seems timely to provide a brief progress report surveying these developments. In addition we discuss an additional set of problems in the hope that these will likewise spur readers to develop further results concerning PPs.

1. Progress Report. We briefly describe some results that have recently appeared and begin by listing two major breakthroughs. We use the same numbering of the problems as in [**16**].

P8. Chowla and Zassenhaus conjecture. *If p is a sufficiently large prime and $f(x)$ of degree ≥ 2 permutes F_p, then $f(x) + ax$ with $0 < a < p$ is not a PP of F_p.*

Cohen [**2**] has affirmatively resolved this conjecture. In fact even better, he proves the following refinement: Let $f(x)$ be a polynomial with integer coefficients and degree $n \geq 2$. Then, for any prime $p > (n^2 - 3n + 4)^2$ for which f (considered modulo p) is a PP of degree n of F_p, there is no integer a with $1 \leq a < p$ for which $f(x) + ax$ is also a PP of F_p. This can be extended to tame PPs over general finite fields. Cohen's proof relies on the deep work of M. Fried in his proof [**8**] of Schur's conjecture which says that every integral polynomial which is a PP mod p

for infinitely many p is a composition of linear polynomials and Dickson polynomials. See also [22] for a recent survey of work on Schur's conjecture.

P9. Carlitz conjecture. *For each even positive integer k, there is a constant C_k such that for each finite field of odd order $q > C_k$, there does not exist a PP of degree k over F_q.*

By resolving singularities of plane curves over F_q, Wan [24] proved that the Carlitz conjecture is true for $k = 2r$ where r is an odd prime. Independently Cohen [3] has obtained the same result through the theory of primitive permutation groups. Cohen also proves the conjecture for each even $k < 1000$.

P2 of [16] asked for new classes of PPs. As a result of his study of factorable and exceptional polynomials over F_q, Cohen [4, 5] discovered the following new class of PPs. Let $L(x)$ be a linearized polynomial of the form $L(x) = \sum_{i=0}^{k} a_i x^{p^i}$ with the property that for some $s \geq 1$, $a_i = 0$ unless s divides i. Such an $L(x)$ is called a **p^s-polynomial**. Let d divide $p^s - 1$ where p does not divide d. Then $L(x) = xM(x^d)$ and $S(x) = xM^d(x)$ is called a **(p^s, d)-polynomial**. If M has no roots in F_q then S is a PP of F_q, see Cohen [4]. As an example, take $q = 2$ and define F_8 as $F_2(\alpha)$, where $\alpha^3 = \alpha + 1$. Then $M(x) = x^5 + (\alpha^2 + \alpha + 1)x + \alpha + 1$ in $F_8[x]$ factors as $M(x) = (x^2 + x + \alpha + 1)(x^3 + x^2 + \alpha x + 1)$ over F_8 into irreducible polynomials. Then $xM^3(x)$ is a PP over $F_{2^{3n}}$ for all integers n with $(n, 6) = 1$.

Wan & Lidl [25] studied another class of polynomials and showed for positive integers d and r satisfying $d|(q-1)$ and $f(x) \in F_q[x]$ that $x^r f(x^{(q-1)/d})$ is a PP of F_q if and only if the following conditions are satisfied: $(r, (q-1)/d) = 1$, $f(\omega^i) \neq 0$ for all $0 \leq i < d$ where $\omega = g^{(q-1)/d}$ denotes a primitive dth root of unity in F_q and g is a fixed primitive root of F_q and $\psi(f(\omega^i)/f(\omega^j)) \not\equiv r(j-i)$ (mod d), for all $0 \leq i < j < d$, where ψ is a multiplicative character with values in $\mathbb{Z}/d\mathbb{Z}$ such that for all $a \in F_q^*$, $\psi(a) \equiv \text{ind}_g(a)(\text{mod } d)$. Here $\text{ind}_g(a)$ is the residue class b mod$(q-1)$ such that $a = g^b$ and $\mathbb{Z}/d\mathbb{Z}$ denotes the ring of integers mod d.

In [9] von zur Gathen gave the following result concerning PPs and polynomials with large value sets. Let $f \in F_q[x]$ have degree $n \geq 1$, $|V_f|$ be the number of distinct images of f so that $|V_f| = |\{f(a)|a \in F_q\}|$, and let $\rho = q - |V_f|$. Then either $\rho = 0$ (so f is a PP) or $4n^4 > q$ or $2\rho n > q$. Hence if q is large and f is not a PP, then either n or ρ is large. See also [11].

P1 of [16] asked for a good algorithm to test whether a given polynomial is a PP of F_q. A probabilistic polynomial-time algorithm to test whether a given polynomial is a PP is given in von zur Gathen [10].

2. More Problems. We list further open problems and continue with the numbering of these unsolved problems from [16].

P10. For $p > 2$ a polynomial f is said to be **planar** if $f(x+e) - f(x)$ is a PP for every $e \in F_q^*$. As indicated in [6, 12, 21] such polynomials are important in the study of affine planes. Clearly any quadratic polynomial $ax^2 + bx + c$ is planar and it is shown in [12] and [21], that if $q > 2$ is prime, then every planar polynomial is quadratic. If $q = p^n$ with $n > 1$ there are planar polynomials over F_q of the form

$$\sum_{i,j=0}^{n-1} a_{ij} x^{p^i + p^j}, \tag{1}$$

where $a_{ij} \in F_q$. Prove or disprove the conjecture from **[6]** that every planar polynomial $f(x)$ with $f(0) = 0$ has the form (1).

P11. Let q be an odd prime, let $1 < k < q - 1$ with $k|(q-1)$, and let $B = B(q,k)$ be the subgroup of F_q^* of order k. Assume that $f, g \in F_q[x]$ are both PPs and suppose that for each $x \in F_q$ and for each $b \in B$,

$$f(x+b) - g(x) \in B. \tag{2}$$

Such a pair (f, g) of PPs determines an automorphism of a design $D(q,k)$, see **[15]**. Conversely, each automorphism of $D(q,k)$ determines a pair (f,g) of PPs satisfying (2). Determine all pairs (f, g) of PPs satisfying (2).

P12. A PP $f(x)$ is called a **complete mapping** of F_q if $f(x) + x$ is also a PP. More generally, for a subset S of F_q containing 0, a polynomial with the property that $f(x) + ax$ is a PP for each $a \in S$ is called an ***S*-complete mapping**, see **[1]**. Complete mappings are useful in the study of orthogonal latin squares. The following conjecture has been proposed by Evans, Greene & Niederreiter **[7]**. If $f \in F_q[x]$ is such that $f(x) + ax$ is a PP for at least $\lfloor q/2 \rfloor$ values of $a \in F_q$, then $f(x) - f(0)$ is a linearized polynomial over F_q where $\lfloor\ \rfloor$ denotes the greatest integer function. By a linearized polynomial is meant a polynomial of the form $\sum_{i=0}^{m} a_i x^{p^i}$ where $q = p^n$. It is known from **[7]** that this conjecture is true for the case $q = p$ a prime and it is true for general q if $f(x) = x^e$. Prove or disprove the conjecture.

P13. Consider the binomial $f(x) = x^k + ax^j$ with $k > j \geq 1$, $\gcd(k, j) = 1$, and $a \in F_q^*$. It is shown in **[23]** that if $f(x)$ permutes F_q then $q \leq (k-2)^4 + 4k - 4$ or $k = sp^r$ with $r \geq 1$ and q is a power of the characteristic p. For $k = 8$, $f(x)$ permutes F_q if and only if

(i) $j = 1$ and $q = 2^{3r}$, $a^{(q-1)/7} \neq 1$ or $q = 29$, $a = \pm 4, \pm 10$,
(ii) $j = 2$, $q = 2^{2r}$, $a^{(q-1)/3} \neq 1$,
(iii) $j = 3$, $q = 11$, $a = \pm 2, \pm 4$,
(iv) $j = 5$ and $q = 4$, $a \neq 1$ or $q = 7$, $a = \pm 3$.

Determine conditions on k, j and q so that $f(x)$ permutes F_q.

P14. If $k > j > i \geq 1$ with $\gcd(k, j, i) = 1$ and $a, b \in F_q^*$ with $a \neq b$, determine conditions on k, j, i and q so that $x^k + ax^j + bx^i$ permutes F_q.

P15. Characterize the PPs over F_q, $q = 2^e$, of the form $h_k(x) = 1 + x + x^2 + \cdots + x^k$. Matthews **[18]** showed that if $q = p^e$, with p odd, then $h_k(x)$ is a PP of F_q, if and only if $k \equiv 1 \pmod{p(q-1)}$. When q is even, this condition is proved sufficient. Such PPs are useful in constructing ovals in projective planes $PG(2, q)$.

P16. Let $q > 2$ be even. Determine all PPs $f(x)$ over F_q with $f(0) = 0$ and $f(1) = 1$ such that for each $a \in F_q$ the polynomial f_a where $f_a(x) = (f(x+a) + f(a))/x$, $f_a(0) = 0$, is a PP. List all such PPs of degrees ≤ 6 similar to Dickson's list of all normalized PPs over F_q. See **[13]**, **[20]** for a connection of these polynomials with hyperovals in $PG(2, q)$, see also **[17**, p. 504**]**.

P17. In **[14]** it is shown that the existence of a j-plane is equivalent to the existence of a very special type of PP. In particular the authors give a construction which shows that if $x^2 + gx - f$ is irreducible over F_q, then there is an associated j-plane if and only if the polynomial $\phi_j(\mu, t) = ft(\mu(\mu + gt) - ft^2)^j$ is a PP for each $\mu \in F_q$. Several classes of j-planes are discussed in **[14]**. Find other classes. Such PPs are related to local PPs studied by Mullen **[19]** where $f(x, y)$ is local if $f(x, a)$ and $f(b, y)$ are PPs for all $a, b \in F_q$.

REFERENCES

1. W.-S. Chou, Permutation Polynomials over Finite Fields and Combinatorial Applications, Ph.D. thesis, Pennsylvania State University, 1990.
2. S. D. Cohen, Proof of a conjecture of Chowla and Zassenhaus on permutation polynomials, *Canad. Math. Bull.* 33 (1990), 230–234.
3. S. D. Cohen, Permutation polynomials and primitive permutation groups, *Archiv. Math.* (Basel), 57 (1991), 417–423 MRj:11145.
4. S. D. Cohen, Exceptional polynomials and the reducibility of substitution polynomials, *Enseignement Mathématique* 36 (1990), 53–65.
5. S. D. Cohen, The factorable core of polynomials over finite fields, *J. Austral. Math. Soc., Series A* 49 (1990), 309–318.
6. P. Dembowski & T. G. Ostrom, Planes of order n with collineation groups of order n^2, *Math. Zeitschrift* 103 (1968), 239–258.
7. R. J. Evans, J. Greene & H. Niederreiter, Linearized polynomials and permutation polynomials of finite fields, *Michigan Math. J.*, to appear.
8. M. Fried, On a conjecture of Schur, *Michigan Math. J.* 17 (1970), 41–55.
9. J. von zur Gathen, Values of polynomials over finite fields, *Bull. Austral. Math. Soc.* 43 (1991), 141–146.
10. J. von zur Gathen, Tests for permutation polynomials, *SIAM J. Comput.* 20 (1991), 591–602.
11. J. von zur Gathen, Polynomials over finite fields with large images, ISSAC-90, Tokyo, Japan, *ACM Press* (1990), 140–144.
12. D. Gluck, A note on permutation polynomials and finite geometries, *Discrete Math.* 80 (1990), 97–100.
13. D. R. Glynn, A condition for the existence of ovals in $PG(2, q)$, q even. *Geom. Dedicata* 32 (1989), 247–252.
14. N. L. Johnson, R. Pomareda & F. W. Wilke, J-planes, *J. Combin Theory Set. A*, A56 (1991), 271–284.
15. W. M. Kantor, 2-Transitive designs, Combinatorics, *Proc. Adv. Study Inst. on Comb.*, Nijenrode Castle, Breukelen, Neth. (eds. M. Hall, Jr., and J. H. Van Lint) *Math. Centre Tracts* 57 (1974), 44–97, Math. Centrum, Amsterdam, 1974.
16. R. Lidl & G. L. Mullen, When does a polynomial over a finite field permute the elements of the field?, *Amer. Math. 'Monthly* 95 (1988), 243–246.
17. R. Lidl & H. Niederreiter, *Finite Fields*, Addison-Wesley, Reading, Massachusetts, 1983 (now distributed by Cambridge University Press).
18. R. W. Matthews, Permutation properties of the polynomials $1 + x + \cdots + x^k$ over a finite field, *Proc. Amer. Math. Soc.*, to appear.
19. G. L. Mullen, Local permutation polynomials over Z_p, *Fibonacci Quarterly*, 18 (1980), 104–108.
20. C. M. O'Keefe & T. Penttila, A new hyperoval in $PG(2, 32)$. *J. Geometry* 44 (1992), 117–139.
21. L. Rónyai & T. Szónyi, Planar functions over finite fields, *Combinatorica* 9 (1989), 315–320.
22. G. Turnwald, On Schur's conjecture, *J. Austral Math. Soc., Series A*, to appear.
23. G. Turnwald, Permutation polynomials of binomial type, *Contributions to General Algebra* 6, Verlag Hölder-Pichler-Tempsky, Wien 1988, 281–286.
24. D. Wan, Permutation polynomials and resolution of singularities over finite fields, *Proc. Amer. Math. Soc.* 110 (1990), 303–309.
25. D. Wan & R. Lidl, Permutation polynomials of the form $x^r f(x^{(q-1)/d})$ and their group structure, *Monatsh. Math.* 112 (1991), 149–163.

Department of Mathematics
University of Tasmania, Hobart
Tasmania 7001
Australia
lidl@hilbert.maths.utas.edu.au

Department of Mathematics
Pennsylvania State University
University Park, PA 16802
mullen@math.psu.edu